VA Information Security Awareness Course

October 1, 2008

Developed by the US Department of Veterans Affairs, Office of Information and Technology, Office of Cyber Security, Education and Training Division

Welcome to the Information Security Awareness Course. This course will take approximately 60 minutes to complete. You are here because Congress mandates that all VA employees, contractors, and all other users of VA information and VA information systems complete computer security training. At completion you will have a deeper understanding of practices that can drastically reduce chances of a security incident happening.

This training focuses on important security practices and procedures. It includes information that VA employees, contractors, volunteers, students Veterans Service Officers, and State Veterans Assistance Office staff need to know in order to protect information about veterans.

If you are taking the paper version of this course, you will need to work with your supervisor and LMS administrator to ensure you receive credit for completion. Additionally, you need to print out and sign the VA National Rules of Behavior at the end of the course. You will need to print and sign two copies of the Rules of Behavior. One copy needs to go to your supervisor and you need to keep the second copy for your own records.

Annual security awareness training is a Federal Information Security Management Act (FISMA) 44 USC 3544(b)(4) requirement. Completion of this course meets the requirement.

Mandatory training related to these laws includes the following required tasks by all VA employees:

Complete Annual Information-Security Awareness Training
Complete Annual Privacy Awareness Training
Read and sign the VA National Rules of Behavior annually

Failure to comply with the above will result in denial or removal of access rights and privileges to VA information and information systems, which may have an adverse impact on the performance of duties.

Upon completion of this course you will:

Know when to contact you Information Security Officer
Know elements required for a secure password
Recognize VA sensitive information
Be aware of information security requirements to protect an individual's privacy
Be aware of the importance of backups
Be aware of the potential dangers of using email
(list continued)
Be aware of the potential danger of using a wireless network
Know how to report suspicious incidents to you ISO
Be aware of how important VA information is to the Government and veterans
Be aware of the difference between the use of VA information resources in your work setting versus for you personal use
Understand the VA National Rules of Behavior

The following topics will be covered in this course:

Know you Information Security Officer (ISO)
Confidentiality
Rules of Behavior
Ethics
Authorized Use of Equipment
Email
Remote Access
Malware
Social Engineering
Public Peer-to-Peer File Sharing
Removable Storage Media
Wireless Network Security
Laptop Security

Passwords
Backups
Incidents

Welcome to the information security awareness course. In the next hour you will review your role in protecting the information of our nation's veterans.

Information Security Awareness helps protect VA information systems. It is more than policies, procedures, rules, and regulations. Information Security Awareness helps you understand what you need to do to ensure:

*Confidentiality, integrity, and availability of veteran's Sensitive Personal Information (SPI)
*Timely and uninterrupted flow of information throughout VA systems
*The protection of VA information and information systems from fraud, waste and abuse

Much of what you learn in this course will not only help you protect VA information, it will also help protect you as a computer user. If you suspect VA information of VA systems have been violated or put in danger (compromised), report this to you Information Security Officer (ISO).
Your ISO is there to help you understand the rules and requirements to keep VA's information and systems secure. Your ISO can help with issues such as:

Knowing what to do if you computer is infected with a virus
Knowing that to do if you see someone using computers inappropriately or for theft or fraud
Understanding your role in protecting the confidentiality and integrity of VA's information
Understanding how backups are conducted and why they are important
Knowing you role in your facility's contingency plan.

Every VA facility has an ISO, who can help you with issues like those above. If you do not know your ISO, ask you supervisor or visit the VA Information Protection Portal for the ISO Directory.

One of your most important responsibilities is keeping VA information confidential

Confidentiality at VA means information is available only to those people who need it to do their jobs. At VA, confidentiality is a must.
To maintain confidentiality:

*Understand what information you have access to and why
*Read and follow remote access security policies
*Only access information systems through approved hardware, software, solutions, and connections.
*Take appropriate steps to protect information, network access, passwords, and equipment
*Control access to patient files or information saved on a disk
*Don't use automatic password-saving features found on web sites
*Promptly report to you ISO any misuse of the remote access process or report if VA sensitive information has been compromised
*Understand that National Rules of Behavior

There are some simply rules that go a long way towards keeping VA's information secure. To maintain confidentiality:

*Lock your computer (Press **Control, Alt,** and **Delete** at the same time, then select **Lock Computer**) when you walk away from it. This will prevent an unauthorized user from performing tasks or accessing information using your account.
*If you print VA sensitive information, make sure you take it from the printer right away and keep it stored in a secure place.
*Protect all information and only access information you need to do you job
*Never talk about a veteran's are in a public place or to anyone who does not have the need to know.
*Never take VA sensitive information home unless you have you supervisor's and ISO written permission.

VA computers are set up to protect confidentiality. But you also have to do your part.

More confidentiality issues arise when it is time to retire old computer equipment. How would you feel if your personal information was stored on a computer, and then the computer was given to another person? This would be a breach of your confidentiality and you wouldn't like it. To prevent this, the VA has strict guidelines in place to ensure that proper sanitization and disposal of media containing VA sensitive information. There is a media destruction project to destroy old or damaged hard drives.

You Information Security Officer or Information Technology (IT) staff should be contacted if you have any media that needs to be destroyed.

Please ensure that information stored on paper or on a computer are properly destroyed before anything is thrown away.

Confidentiality Tips:

*When possible, store information on your facility's network drives- not your desktop computer
*If you see computers being excessed without full data erasure, let your ISO know.
*Understand the concept that clicking on the **Delete** button doesn't really delete a file completely from your computer
*Follow you local policies and procedures for disposing of printed copies containing sensitive information by contacting your ISO for media destruction procedures. These documents should be shredded using an NSA approve cross-cut shredder. More information of the destruction of paper records can be found in VA Directive 6371, Destruction of Temporary Paper Records.

Ethics is about what is right and what is wrong. This goes beyond legal obligations and deals with actions that affect other people.

Ethics
Ethics deals with what is right and wrong. Within VA, ethics needs to be focused on providing the best health care, benefits, and services for our nations' veterans. Applied to our computing practices, this means we need to ensure we are operating our computers in a manner that supports that VA's mission. Taking this a step further, we need to also make sure we implement appropriate computer practices and do not do anything that could introduce problems into the VA's computer network to tarnish our reputation. If a mistake is make that could affect this, it is ethical to bring this mistake tour supervisor's and ISO's attention as soon as possible to prevent the issue from causing additional harm.

A quote in the area of ethics is "Proper ethics is what we practice, so we can have peace of mind and be able to sleep at night".

Authorized Use of Equipment
In some situation, you may have limited personal use of certain government resources.

The American people, especially our veterans, expect us to protect their information. They also expect us not to abuse or misuse the resources provided to us to accomplish our mission. As a VA employee, you may have the privilege of some "limited personal use" of certain Government resources, such as computers, email, Internet access, and telephone/fax service.

Some locations permit employees limited use of equipment. If this is the case at your facility, check the guidelines to make sure you do not violate what is allowed.

Limited Personal Use
This benefit is available only when it:

*Does not interfere with official VA business
*Is performed on the employee's "non-work" time
*Involves no more than minimal expense to the Government
*Is legal and ethical

These benefits may be limited or eliminated at any time, especially if you abuse these privileges. Restrictions for personal use of resources can vary between VA facilities. To protect yourself, you should discuss your limits and responsibilities with your supervisor and ISO. More can be read about limited personal use of government equipment in VA Directive 6001, Limited Personal use of Government Office Equipment Including Information Technology.

There are many examples of inappropriate use of government resources.

Inappropriate Use

Examples of misuse or inappropriate use are:

*Any personal use that could slow down, delay, or disrupt Government systems or equipment. These include continuous data streams, video, sound, chain letters or other large files which slow down the VA network

*Using VA systems to get authorized access to other systems

*Activities which are illegal, inappropriate, or offensive to fellow employees or the public. These include hate speech or material that ridicules other because of their ace, creed, religion, color, sex, disability, national origin, or sexual orientation.

*Creating, downloading, viewing, storing, copying, or transmitting sexually explicit or sexually oriented materials

*Creating, downloading, viewing, storing, copying, or transmitting materials related to gambling, illegal weapons, terrorist activities, or any other illegal or prohibited activities

*Using Government systems or equipment to make money, to get a non-government job, or do any business activity (for example, consulting for pay, sale or administration of business transactions, sale of goods or services)

*Posting VA information to external newsgroups, bulletin boards, or other public forums without permission. This includes any use which may make someone else think the information came from a VA official (unless approval has been obtained), or uses that are at odds with the Agency's mission or position

*Any use that could cost the Government money

*Accessing, using, copying, or sending VA computer software or date, private information, or copyrighted or trademarked information without permission

If you have any questions about whether an action would be considered inappropriate ask your ISO and Supervisor. Be sure to discuss your limits and responsibilities with your supervisor and ISO.

Email Privacy and Security

Email is a great tool that we have become dependent upon to perform our jobs. However, we need to use it appropriately to protect our veterans' information and take certain precautions to reduce the risks of spreading viruses.

Electronic mail (email) helps us do our jobs faster, but using email also has risks.

Email isn't like a personal letter delivered to you in a sealed envelope by the post office. Instead, email is more like a postcard that gets dependably delivered, with opportunities along the way for other people to see what is says. Since email is **not private**, never use email to send VA sensitive information about veterans or employees unless it is encrypted. If a work related issue requires you to send sensitive personal information (SPI) about a veteran or VA employee in an email message, you are required to encrypt the message (encrypt with PKI or RMS). Using PKI to encrypt a message validates that the message is authentic, keeps it confidential, and protects the message content from being altered.

Chain letters and hoaxes are message that waste our time and slow down VA's network. Don't participate in forwarding either of these to other computer users.

Chain letters and hoax messages slow down VA's network. This type of email clogs up the network and may contain dangerous code. **NEVER** forward or reply to these messages. **DELETE** them, preferably without opening them. If you accidentally open the email, close it and delete it. **NEVER** open any attachments that come from an unknown source. Also, never reply by saying, "Please stop" it slows down the VA's email system.

Safe email practices go a long way to prevent information security issues from arising. The old adage of "An ounce of prevention is worth a pound of cure" has proven to be very true in the information security world.

Email Hints

Here are a few tips on using email safely:

*Use virus protection software, and keep it up to date
*Make sure your virus protection program scans all emails and attachments you send or receive
*Learn to recognize the signs of a virus infection
*Additionally, since most computer viruses are spread by email, do not open email attachments that are from people you do not know

*Never open emails with inappropriate subject lines
*Use "Reply to All" sparingly. Does everyone in your large email group really need to see you response? Often, it's more appropriate to limit you responses to just the sender.
*Replying to unsolicited spam email is actually more likely to increase the number of messages sent to your address. When spammers receive a reply, the reply tells them you email address is valid.
*Don't forward of create hoaxes or ask people to modify their computer systems.
*Don't spread rumors using emails. Be suspicious of any message that tells you to forward it to others.

*Don't participate in "mail-storms". You don't need to send a message saying "me too" or "thanks" or ever "please stop"
*Don't open attachments from senders you don't know
*Don't expect privacy when using email to transmit, store, and communicate information.

Always remember that email is not a private communication tool. If you have any questions about how to deal with spam or how to encrypt a message, talk to your ISO.

Remote Access

Remote access provides users that are traveling with the ability to work while they are on the road. If you use remote access, make sure that you follow VA policies to ensure that VA's sensitive information is protected. Safety in this area includes obtaining permission from your supervisor and ISO before connecting remotely, not sharing VA information or passwords, and not removing VA sensitive information from VA's protected environment without supervisor and ISO's permission.

You are only allowed to access, use, or send VA sensitive information while off-site if you have the permission of your supervisor. Also, you can only do so when the following security steps have been taken:

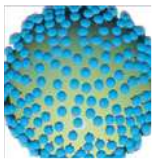
*You can only access, use, or send VA information from a VA-owned laptop, handheld computer, or storage device unless you have a waiver from the CIO. You must have your supervisor's permission to obtain remote access.
*You must apply for this permission through your ISO
*You must have your supervisor's permission to transport, transmit, access, and use VA sensitive information outside of VA facilities
*You cannot share VA information with anyone else
*You must not share you username or password- or instructions on how to access the VA network- with anyone else.

Removable storage media may be convenient, but in order to use it certain security requirements must be followed. All removable storage devices that connect to VA's resources via USB ports (thumb drives, external ports, etc) must be encrypted with FIPS 140-2 approved encryption.

In order to store VA sensitive information on removable storage media, you must have permission from your supervisor and your ISO. Only VA approved and procured thumb drives are allowed within VA. VA sensitive information outside of VA's protected environment must be encrypted.

If you require a USB drive to complete your job, you will need to obtain written permission from your supervisor and your ISO.

VA Handbook 6500 requires written permission from both your supervisor and designated Information Security Officer (ISO) to obtain a thumb drive.



Malware

Malware are dangerous programs, written with malicious intentions to either harm or steal information. Viruses are one of the many different malware programs that could infect your computer equipment.

High-tech vandals have created dangerous programs that infect computer systems. These programs vary in how they infect and damage systems and are collectively called "Malware". When our systems become infected with malware they may not operate properly.

Worms are malware viruses that replicate over and over again. The intention of a worm is to tie up computer and network resources so that users will have a difficult time working and communicating. Worms have had a history of causing problems and worms such as Code Red caused the Internet to slow down on a global basis.

Viruses
Viruses are one type of malware that attack computers. Viruses find their way into computers by attaching themselves to files that are downloaded or transferred between computers. They can be spread many ways- from a CD, DVD, removable storage devices, web site, or email. It takes time and money to defend against viruses.

Worms
Worms infect systems and then replicate themselves. They are a simple virus that can make a copy of itself over and over again. A worm can be dangerous because it quickly uses all of the available memory on your system and brings it to a halt. Viruses that can get around VA protections and attack one computer after another are even more dangerous.

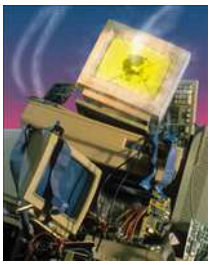
Malicious email
Malicious email hoaxes are not viruses but they can still be dangerous. In most cases, the sender asks you to forward a warning message to everyone you know. A good example of a hoax is one that has a subject line saying "Delete this file immediately". The message tells you how to locate a computer file and delete it. A hoax may offer a way to help you fix a problem, but when you do what it asks, it actually disables your system. Even harmless messages, can still cause problems. Harmless messages forward to many other people slow down the VA network, which also slows down the process of serving America's veterans.

Trojan Horses
Another type of virus is a Trojan horse. The term "Trojan horse" comes from the story in Homer's Iliad. The ancient Greeks gave a giant wooden horse to their enemies, the Trojans, as a peace offering. After the horse was moved inside Troy's city walls, Greek soldiers came out of the horse's empty belly and opened the city gates. This allowed more soldiers to enter Troy and destroy it. These programs may seem harmless. Even though they do not replicate themselves, they can be just as destructive as viruses and worms. Their mission is to get destructive viruses into computers and networks.

Your computers have antiviral software installed on them. This software is maintained by your computer administrators. VA uses a Department-wide antivirus program. Antivirus software is automatically installed and updated. However, new viruses are developed every day. They can be spread from inside or outside VA. There is no protection from newly discovered viruses. That's why it is important for you to protect yourself and the VA.

Odd computer behavior can be a sign of malware. There may be a problem if your computer has any of these symptoms:

*Reacts slower than usual
*Stops running for no apparent reason
*Fails to start ("boot")
*Seems to be missing important files
*Prevents you from saving your work



Here are a few tips to help you deal with malware. As with most information security practices, prevention goes a long way. Here are a few tips:

*Delete email messages from unknown senders or messages with unusual subject lines, such as "open this immediately".
*Never stop or disable you antiviral program
*Make sure your files are backed up on a regular schedule. Check with your IT staff to ensure your information is being locked up.

Email attachments and clicking on links inside of email are a very prominent way in which malware can infect your system. This is why our email should not be abused.

Set you virus protection software to scan your email and attachments
Be very careful if someone sends you an attachment containing executable code. You can recognize these by the file extensions, such as: .exe, .vbs, .js, .jse, .wsf, .vbe, and .wsh

Do not delete any system files when asked to do so in an email; report this to your ISO.

Having up to date antiviral software installed on your computer is essential in protecting your system and the VA network from an infection. If you have any doubt that the antiviral software installed on your computer is up to date, contact your IT staff or ISO.

Malware Summary
All VA computers must have virus protection software. To work properly, virus protection must be kept up to date. New updates are issued nearly every day. Contact your ISO or Information technology staff if your VA computer is not up to date. While many sites automatically update virus protection software on network computers, some systems are not updated automatically. It is critical to update your antiviral protection regularly.

To learn more about computer viruses and your role in viral defense, talk to your ISO.

Social Engineering

With well protected networks, hackers or crackers have a hard time breaking in using technological approaches. In these cases, they will resort to social engineering and depend on people's kindness or sense of trust to steal information or resources.

What is Social Engineering
Social engineering happens when a person tries to gain your trust in order to get information and resources which he or she can use to harm. This is an important security issue!

Social Engineering Methods
A Social Engineer may try to trick you into giving them your password to illegally gain access to your system or information about VA's patients, beneficiaries and dependents, and employees. We know you want to be helpful, but social engineers may try to take advantage of your kindness.

If people ask you for VA sensitive personal information (SPI), make sure you know who they are and if they really need access to the information. Also, make sure they have permission to get such information or access it as part of their job.

If someone asks you for something that seems unusual, contact your supervisor before proceeding. A social engineer posing as an IT specialist can gain access to a lot of resources if you give them your password.

One example of social engineering that hurt a VA facility was a phone call from someone claiming to be from the "phone company". The thief said he was testing lines and long distance circuits. The thief then asked an employee to dial a special code, which gave him access to a long distance service. This scam resulted in thousands of dollars worth of unauthorized calls being made at VA's expense.

You are the first line of defense. As we learn more about the tactics hackers use to get access to VA's information and computer systems, hackers continue to look for new ways to get around our protections. Social engineers will rarely ask for sensitive information directly, but will work on gaining your trust and manipulate you into assisting them in getting the information and resources.

You have to be diligent in protecting the VA from the tactics of social engineering because you are our first line of defense.

Public Peer-to-Peer File Sharing

Peer-to-Peer file sharing can cause major security issues within the VA and is prohibited.

Public Peer-to-Peer file sharing (commonly known as P2P) refers to programs that let anonymous files be shared between computers. There are times when using P2P is helpful. But most of the time, these programs break the law by sharing copyrighted music, videos, and games. Some common public P2P programs are Kazaa, Freewire, Grokster, and Morpheus.

Public P2P is not allowed at VA.

Please protect our computers by not using Peer-to-Peer file sharing.

P2P programs also can be used to spread viruses and "spyware". Spyware programs track what you do on your computer and send information to thieves and hackers- without you knowing it. For example, someone could use spyware to get information about you, your coworkers, veterans, and veterans' families. This information could be used to steal your identity, buy items on a veteran's credit card, or collect personal financial information about a VA employee. In addition, P2P file-sharing makes the VA network run slower.

Don't be a victim. Use your computer wisely. If you think your computer may have P2P software of spyware, tell your ISO.

Wireless Network Security

Due to wireless technologies' convenience, it is being used by many federal agencies. An important item to note here is that the only time a computer is permitted to connect to the VA network wirelessly, is if the connection is encrypted using a FIPS 140-2 validated method.

Wireless Networks and the VA
If you use a wireless network, it si important you know how to use it safely and know the potential consequences if you don’t. Wireless networks, which use radio waves to transmit date, are being used more often by Federal agencies. They allow users to do their work while moving around from one location to another. Poorly controlled wireless networks can allow sensitive information, passwords, and other information to be read, changed, or transmitted by unauthorized users. If a wireless local area network is set up, it needs to be encrypted using a FIPS 140-2 validated method.

Improperly used wireless technologies can introduce a multitude of vulnerabilities to the VA's network. If you are using this technology be aware of the potential issues and take all necessary precautions.

Wireless Dangers
Here are some examples of the dangers associated with wireless networks:

*Another person can eavesdrop on a transmission between two workstations (e.g, a wireless PDA and a base station)
*An attacker can analyze traffic and learn more about an organization's communication patterns, such as days or times personal information is sent from one employee to another.
*By intercepting your logon information via eavesdropping on a transmission, an attacker can pretend to be you to get access to private information, to change data, or to send it to someone else.

In many cases wireless networks can assist us in completing our jobs. If you are a user of a wireless network, please take extra precautions to protect our networks.

More Wireless Dangers

*An attacker can become "the man in the middle" by intercepting messages, stopping them from being sent, or transmitting them to someone else
*An attacker can change or delete a message
*An attacker can jam a wireless network with extra radio signals to stop you from accessing information. Other devices such as cordless phones or microwaves can prevent a wireless network from working properly.

If you use a wireless network, contact your ISO to learn more about how you can do your work safely.

Laptop Security

Laptops are very useful tools in today's computing world. If you use a laptop you can protect the information on it by; ensuring that the hard drive is encrypted, making sure that antiviral and other software updates are installed, and practicing physical security techniques.

Protection of data stored on laptops is a very important component in securing our veterans' data. Laptops can contain large amounts of data that could fall into the wrong hands if proper precautions are not taken. The following list can assist in protecting the data on laptops:

*Ensure all data on the hard drive is encrypted
*Make sure your system administrator maintains your laptop and all the latest software upgrades are installed. This includes antiviral software, personal firewalls, software patches, and Virtual Private Network (VPN).
*Physically secure your laptop. His includes keeping it close to you while traveling and using locking cables if you must leave it in a hotel room.
*Taping contact information such as a business card to the bottom of a laptop could aid in recovery, if it is lost or stolen.

Passwords

Passwords are an essential part of any security program. To so your part in protecting the VA's information, you must protect your password. This means that you mus have a strong password that is not shared with anyone.

Importance of Passwords
Passwords are important tools for protecting VA information and information systems and getting your job done.

They ensure that you and only you have access to the information you need. Keep you password secret.

If you have several passwords, store them in a safe and secure place that no one else know about.

Strong Passwords

Strong passwords have at least 8 characters, include upper and lower case letters, number, and special characters. VA requires strong passwords on all information systems. Passwords must:

*Be changed at least every 90 days
*Have a least eight characters (i.e. Gabc123&)
*Use at least three of the following four kinds of characters:
-Upper case letters (ABC…)
-Lower case letters (…xyz)
-Numbers (0123456789)
-Special characters, such as #&* or @

Using these rules will provide you with a "strong" password.

When hackers or crackers attempt to break into computing systems using passwords, they begin with common everyday words. They actually use lists of dictionary words and names in automated password cracking tools. Other ways they try to crack passwords is by using birthday, social security numbers, and addresses. To ensure that you are using strong passwords stay away from using any of these items.

Passwords Rules of Thumb

*Don't use words found in a dictionary
*Follow the rules for strong passwords
*Don't use personal references (names, birthdays, addresses, etc)
*Change your passwords at least every 90 days. If you suspect someone may know your password, change it immediately and inform your ISO
*Never let anyone stand near you while you type you password. Ask people to turn away while you type it, and don't let them see your keyboard while you type
*If you have several passwords to remember **you may** write them down, but keep them in a locked place so no one else can get to them.

Strong passwords can be developed by using parts of each word in a phrase. This in combination with numbers and special characters can help you develop a strong password that is easy for you to remember.

Remembering Passwords
Since childhood, many people have used simple rhythms to remember things. Can you remember how you learned the alphabet, months of the year, state capitols, etc.? Sometimes people use "mnemonics", which are things such as formulas or rhymes that help with memory.

Below is an example of a mnemonic used to remember the planets of our solar system: "**M**y **V**ery **E**xcellent **M**other **J**ust **S**erved **U**s **N**ine **P**izzas" This helps you remember the names and order of the planets.

Mnemonics can help you develop and remember strong passwords.

Remembering Passwords
Another sample mnemonic: **M**ercury, **V**enus, **E**arth, **M**ars, **J**upiter, **S**aturn, **U**ranus, **N**eptune, **P**luto

It may sound silly but it works. A simple mnemonic just needs to make sense to you. Mnemonics are a useful tool in constructing passwords that cannot be found in the dictionary. How about using this as a passwords for the mnemonic above:
MVEMJS,unp

For more information about passwords, ask your ISO.

As mentioned earlier, strong passwords are en essential part of any information security program. In order to do your part, do not share your password with anyone. This would compromise the VA's security and possibly cause issues for yourself.

Protecting your Password
Your username and password protect you and the information stored on VA computers.

When you log into a VA system, the combination of your user name and password indentified YOU as the person accessing the system and information. All actions taken after you log into the system are identifiable back to you, so it is important that you **NEVER** share your log in information.

If someone else uses your account information, you are responsible. Guard your password and never disclose it to anyone!

Backups
Backing up your information is an essential part of protecting VA information. We must always remember that computers are mechanical equipment and that all mechanical equipment will eventually fail. Therefore the information stored on your local hard drive, also needs to be stored someplace else such as a drive mapped to a server.

Importance of Backups
Any work you do on the VA's computers is important. It is important to you because of the time and effort expended to create it. It is important to VA and to veterans because it supports our mission. There are some resources we can't afford to lose, so database backup are systematically and routinely created on systems such as VistaA, BDN and others. Backups are cheap insurance. Backing up data is an important step to protecting your hard work.

Backup Routines
VA information technology staff work hard to make sure the VA data is safe and routinely backed up. Most facilities have routines that automatically backup on users' computers to a networked server in a computer room.

The question is not **if** you will ever need to use you backup- the question is **when;** so making backups is a smart practice for your home computer, too.

Information that resides on your computer is very valuable and it needs to be backed up. Consider all the hard work that you have done to complete those documents. You would not want a hardware failure to ruin weeks or even months of your hard work.

Your Role for Backups
What you can do to assist in this matter is:

> Keep your files in one location, such as the "my Documents" folder or mapped network drive. This will make it easy to find and create backup files.
>
> If you ar a remote user or travel a lot, you should check with your IT staff to ensure your data is being backed up.

If you have any concerns about how your system is being backed up, contact your IT staff or ISO.

Incidents
Unfortunately information security incidents do happen. However, your response during one of these incidents can prevent it from blowing up into something out of control. For instance if a new virus that could harm all the computers in the VA hits your computer first, your prompt response could prevent a catastrophe. By notifying your IT staff and ISO of such an incident, they could take proper actions.

Dangers of Incidents
You know how important computers are when we are doing our jobs. At VA, so much of what we do depends on our computers. Security incidents include the following:

A virus attack
A lost or stolen computer
Files are missing or were compromised
Sensitive personal information (SPI) was shared with people who do not have a need to know

All of these are examples of computer-related incidents. It is important to tell your supervisor and ISO when you see such incidents.

Possible Incidents
Leakage of sensitive data is one of many possible incidents. This list below include possible incidents that could occur.

*A stranger is sitting at a VA computer, whom you believe has no authorization to be there.
*A veteran's personal medical information id left unattended on a desk, a copier, or a computer screen.
*A co-worker sends a patient's sensitive personal information (such as a combination of a full name and social security number or account number) to an outside e-mail address- even is it is the patient's personal physician- via unencrypted email.
*You discover an open box with reams of computer print-outs containing sensitive personal information standing unattended by a dumpster.

If you think an information security incident has occurred, you should gather information about what happened and report it to your ISO and supervisor immediately. This should be done by calling them or reporting it in person. It is not your duty to report this to the press or other individuals outside of the VA.

Incident Do's and Don'ts

If you think a security incident has occurred, you should:

*Write down the date, time, and location the incident took place as well as the which may have been affected.
*Tell your ISO and Privacy Officer what happened.
*Write down any error messages that showed up on your computer screen
*Write down any Web addresses, server names, or IP addresses involved in the incident.

Protect Yourself

If you witness what you believe to be a security or privacy incident, you are obligated to report it immediately to your facility/office ISO, Privacy Officer (PO) and /or supervisor. If you fail to report such an action, you may be considered an accomplice to that action.

Loss or theft of portable equipment has significantly grown and is a major cause of security breaches. These data breaches violates our promise to our Veterans and put them at risk for identity theft.

Incident Do's and Don'ts

You've probably heard about the theft of electronic information from the VA employee's home. The data included names, addresses and social security numbers of millions of veterans. Fortunately, the information was recovered and was never accessed.

So, when you suspect an incident may have occurred, it's very important you tell you ISO, Privacy Officer and supervisor immediately (i.e. one hour or less). Don't wait.

It's best to contact you ISO/PO in person or by telephone rather than by email. You may **not** contact the media (radio, TV, newspapers) or anyone outside your VA facility. If a crime is involved, (such as an item was stolen) you also need to report it to VA law enforcement. VA Handbook 6500.2, Managing Security and Privacy Incidents, provides additional procedure on incident management.

Rules of Behavior
The VA National Rules of Behavior you sign in order to access VA information and information systems clearly states your information security responsibilities.

What are the VA National Rules of Behavior:
Everyone who access VA's information and information systems must understand their security roles and responsibilities.
Information security do's and don’ts are established in a document known as "VA's National Rules of Behavior"
Prior to being granted access to VA's information and information systems, users must agree to the VA National Rules and Behavior, stating they have read, understand, and will abide by these security rules.
The VA National Rules of Behavior must be read and signed each year.
The VA National Rules of Behavior also contains the consequences of inappropriate behavior.
Consequences may range from a written reprimand to losing your job, depending upon the violation.

Rules of Behavior ensure everyone is aware of their security responsibilities and helps to protect our veteran's data

More on VA's National Rules of Behavior

*Rules of Behavior ensure everyone is aware of their security responsibilities and helps to protect our veteran's data.
*ISO's are available to explain and provide clarification to anyone who needs assistance understanding ROB.
*Additionally, VA employees are responsible for protecting Personally Identifiable information. VA Directive 6600, Responsibility of Employees and Others supporting VA. In Protecting Personally Identifiable Information (SPI), requires all employees to treat sensitive information of others the same as they would like theirs treated.
*A computer based training (CBT) module is available for users explaining the VA's National Rules of Behavior- contact your ISO for more information.

Read VA Directive 6600

The next page will take you to the VA National Rules of Behavior. Please read, acknowledge, and accept the Rules of Behavior.

The last pages in this course will provide you with the **VA National Rules of Behavior.** You will need to sign the Rules of Behavior in order to be able to receive credit for completion of this course. Provide a signed copy of the Rules of Behavior to your supervisor and make a copy for yourself.

These rules serve to provide notice of what is considered acceptable use of all VA information and information systems, VA sensitive information, and behavior of VA users.

Final Summary

The VA and our nation's veterans are depending on you to do your part in information security protection. Keep in mind that our information and information systems also assist with our readiness during national emergencies. Your safe practices can protect VA information and contribute greatly toward providing our Veterans with top quality services. This will benefit you, the Veteran, the VA, and our nation. Thank you for doing a great job in this area.

VA's information and information systems are a major part of how we help veterans. They also affect our readiness to work with other Federal agencies, such as the Departments of Defense, Health and Human Services, and Homeland Security, during national emergencies.

The FBI has warned all Federal agencies that their systems, and the information in those systems, are potential targets for attacks. Now more than ever, VA's systems and the information they contain must be available to serve our Nation and its veterans. Please be careful. Don't do anything that might damage our information and information systems.

The work we so at the VA is an important part of our Nation's security and this puts VA's information systems at risk. VA employees must do their part to prevent attacks that would breach the security of the systems and the information that could interrupt care of our veterans. You have just learned some important information that will assist you with guarding information and what steps to take if a breach occurs.

Remember, if an incident occurs report it to your ISO and PO immediately. If your ISO is not available, contact your Network ISO.

Self Test for Information Security

Name: _____ Date:_____

Question 1

If you believe a security risk has occurred you should:

A. Not do anything about it
B. Inform you ISO
C. Contact the news media
D. All of the above

Question 2

If you are working with medical data and you find interesting medical information about a neighbor, you should:

A. Obey VA's confidentiality principles and not share the information with anyone except on a need to know basis for work related purposes
B. Tell your other neighbors, but make sure that they promise not to tell anyone
C. Print it out and take it home, as long as you don't share it with anyone
D. Download the information to your personal USB flash drive

Question 3

Which of the following is considered inappropriate use of government resources?

A. Running a side business
B. Applying or a VA job during your lunch break
C. Gambling
D. Visiting a news web site during a break
E. Choice A and C
F. Choice B and D

Question 4

What should you do if you receive an email attachment from someone you don't know?

A. Open the attachment if the subject line seems harmless
B. Reply to the email and ask for more information
C. Do not open the attachment
D. Open the attachment if your virus software doesn't tell you not to.

Question 5

Which of the following are appropriate security steps when working remotely?

A. Not sharing VA data with anyone outside the VA
B. Obtaining your supervisors permission
C. Not sharing you username and password
D. Not storing VA sensitive data on you system without appropriate approvals and encryption
E. All of the above

Question 6
Software specifically designed to damage, corrupt, and disrupt a computer or network is known as:

A. My Favorites
B. Malicious software or "malware"
C. Junk mail
D. Spam

Question 7
If you think your computer is infected with a virus, you should tell:

A. Your computer manufacturer
B. Your Information Security Officer (ISO)
C. Acme Virus Protection, Inc.
D. Your supervisor
E. None of the above

Question 8
Social engineering is a way for people to gain your trust so they can get you to give them information or access to VA resources they shouldn't have

True
False

Question 9
Practices that contribute to secure laptop usage include:

A. Encrypting the hard drive
B. Ensuring that the systems administrator is keeping the laptop updated
C. Keeping the laptop protected while traveling
D. All of the above

Question 10
Which of the following are secure password practices?

A. Using upper case, lower case, numbers, and special characters
B. Using words found in the dictionary
C. Using names, birthdays or locations
D. Using social security or license plate numbers

Question 11
Which of the following items are recommended for backing up your files?

A. Store files in a single location such as the My Documents folder
B. Computers are mechanical equipment which can fail. Therefore you data should be backed up on a regular basis
C. If you are not sure your backups are occurring regularly, contact your IT staff
D. All of the above.

Question 12

If you think a computer security incident has occurred, you should:

A. Ask your friend down the hall what to do.
B. Gather all the information you can, and report it to your ISO and PO
C. Contact the local media
D. All of the above

Question 13

Which of the following are rule violations that should be reported?

A. A co-worker sends a patient's sensitive personal information to the patient's physician outside email address via an unencrypted email
B. A stranger who you believe has no authorization to be there is sitting at a VA computer
C. A veteran's personal medical information is left on a desk, copier or computer screen where unauthorized individuals can see it.
D. All of the above.

Reference Page

VA Directives

VA Directive and Handbook 6500, Information Security Program
VA Directive 6300, Records Information Management
VA Directive 6301, Electronic Mail Records
VA Directive and Handbook 0710, Personnel and National Information Security

Federal Policies

Federal Information Security Management Act (FISMA) Title III, 2002 E-Gov Act
OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources
Health Insurance Portability and Accountability Act of 1996 (HIPPA)
Clinger-Cohen Act of 1996